Feedback on EDPB Guidelines 02/2026 on Anonymisation (version for public consultation)

v 1.0 · 30 October 2026

1. Introduction
2. GL § 15: the processor rule should be revised
   - 2.1 The rule laid down in GL § 15 is inconsistent with other parts of the Guidelines
   - 2.2 The rule has no basis in SRB and conflicts with SRB §§ 86 and 89
   - 2.3 The rule is incompatible with the text of the GDPR
   - 2.4 The teleological argument does not support the rule
   - 2.5 The rule makes pseudonymisation pointless
3. Conclusion

1. Introduction

This feedback is submitted by Paolo Maria Gangi, LL.M., data protection officer and lawyer admitted to the Rome Bar (avvocato), in response to the public consultation on the EDPB Guidelines 02/2026 on Anonymisation, version 1.0 adopted on 7 July 2026 (the "Guidelines").

This feedback concerns essentially one provision of the Guidelines, GL § 15. The author respectfully submits that the rule laid down in GL § 15 should be reconsidered: an entity that processes, on behalf of a controller, pseudonymised data whose key it does not hold and cannot obtain (hereinafter the "Pseudonymised Data Handler") should not, in the author's view, be regarded as a processor of personal data. That conclusion appears to follow from the judgment of the Court of Justice of 4 September 2025 in Case C-413/23 P, *EDPS v SRB* ("SRB"), from the Opinion of Advocate General Spielmann of 6 February 2025 in the same case (the "Opinion"), from the text of the GDPR itself, and finally from practical considerations regarding the consequences of the rule. The reasons are set out in section 2 below.

References to paragraphs of the Guidelines are marked "GL §"; to SRB "SRB §"; to the Opinion "AG §". SRB was delivered under Regulation (EU) 2018/1725, whose

Via G.G. Belli n.39, 00193, Rome, Italy – VAT: 15655341004
Tel.: +39 06 92963036 – email: info@gangitechlaw.com
www.gangitechlaw.com

definitions the Court holds must be interpreted in the same way as those of the GDPR (SRB § 52): references to the GDPR below therefore apply equally to that Regulation.

2. GL § 15: the processor rule should be revised

GL § 15 provides that *"if an entity processes information on behalf of another, whether the given data is personal for that entity should be assessed by reference to the controlling entity's perspective"* and that *"in practice, this means that if an entity processes information on behalf of a controller (i.e. someone for whom the information is personal data, and who decides the purposes and means of the processing), that information should also be considered personal data for the processing entity"*. It concludes that *"that entity should, therefore, be considered a processor under the GDPR and be subject to the obligations applicable to processors"*. This is exactly the SRB situation: under GL § 15, Deloitte would be a processor simply because the SRB is a controller, and Example 3 of the Guidelines follows the same line of reasoning.

The author of this feedback submits that the rule should be rephrased, for the five reasons set out in sections 2.1 to 2.5.

2.1 The rule laid down in GL § 15 is inconsistent with other parts of the Guidelines

The glossary of the Guidelines defines an entity as a party that, *"depending on whether or not the information is personal"*, could be *"a potential controller, a potential processor, or a potential third party"*. GL § 4 states that it is not possible to know whether the person holding the data should be described as a controller, *"since that answer will depend on whether the data being tested is personal or not"*. GL § 37 accepts that information may be *"anonymised for the entity which receives the given data, but not for the anonymising controller"*.

In all the above passages the role of processor follows from the nature of the data. GL § 15, however, reverses that order: the mere fact of acting on behalf of a controller is taken to determine the nature of the data. Read together, the above passages appear difficult to reconcile with GL § 15, and the author respectfully suggests that the approach reflected in the glossary and in GL §§ 4 and 37, which is also the one consistent with SRB, should prevail.

2.2 The rule has no basis in SRB and conflicts with SRB §§ 86 and 89

GL § 15 does not cite any paragraph of SRB in support of the rule it lays down. The only justification given is that the rule *"follows from a teleological application of the GDPR"*, a reasoning that is examined, and respectfully questioned, in section 2.4 below. The text of SRB points in the opposite direction, for three reasons:

- SRB § 86 states that *"pseudonymisation may, depending on the circumstances of the case, effectively prevent persons other than the controller from identifying the data subject in such a way that, for them, the data subject is not or is no longer identifiable"*. The Court makes no exception for persons acting on the controller's behalf. Deloitte worked at the SRB's request: the SRB *"asked Deloitte, in its capacity as independent valuer, to assess the relevant comments relating to Valuation 3"* (SRB § 21). The Court nonetheless assessed the data from Deloitte's own perspective and by reference to Deloitte's own means, asking whether Deloitte was *"in a position to lift those measures"* and whether the measures prevented Deloitte *"from attributing those comments to the data subject including by recourse to other means of identification such as cross-checking with other factors"* (SRB § 77). The Court did not transpose the SRB's perspective to Deloitte because Deloitte worked for the SRB.
- SRB § 89 states that Regulation 2018/1725 *"contains obligations, such as the obligation to provide information to the data subject …, compliance with which requires the data subject to be identified"*, and that *"such obligations cannot be imposed on an entity which is in no way in a position to carry out that identification"*. GL § 15 does exactly what the Court says cannot be done: footnote 12 of the Guidelines lists the obligations it imposes on the processor (Articles 27, 28, 29, 30(2), 31, 32, 33(2), 37, 38, 44, 46, 48 and 49(6) GDPR), and several of them can only be performed by an entity that knows whose data it holds: assisting the controller with data subject requests (Article 28(3)(e) GDPR), notifying personal data breaches (Article 33(2) GDPR), keeping a record of the categories of data subjects (Article 30(2) GDPR). An entity for which the data are not personal cannot, by definition, perform them. Section 2.3 below develops this point further.
- GL § 15 revives the argument the EDPB made as intervener before the Court, namely that under the General Court's approach *"personal data change in nature when they are transmitted to an entity outside the controller, which does not have the additional information enabling the data subject to be identified"*, and that this *"would allow such a controller unduly to remove personal data from the scope of EU law on the protection of such data, even where the processing by the external entity would expose the data subjects to significant risks"* (SRB § 64). The Court answered that argument directly: *"the EDPS is incorrect in so far as he submits that the fact that pseudonymised data are not, as the case may be, personal in nature for persons to whom the controller transfers the pseudonymised data makes it unduly possible to remove those data from the scope of EU law on the protection of personal data"*; the reason is that *"that fact has no bearing on the assessment of the personal nature of those data in the context, inter alia, of a potential subsequent transfer of those data to third parties"* (SRB § 85). As to the objective of a high level of

protection, the Court held that the concept of personal data *"is not unlimited since that provision requires, inter alia, that the data subject be identified or identifiable"* (SRB § 88). The complaint was *"rejected as unfounded"* (SRB § 90).

In the author's respectful view, therefore, the reasoning of the Court in SRB not only does not support GL § 15 but appears to point in the opposite direction.

A final observation on the SRB case may be useful. The view expressed in this feedback, namely that GL § 15 should be revised, does not entail any lowering of the level of protection afforded to data subjects, nor any reduction of the controller's obligations towards them. The controller that processes personal data retains the full set of its GDPR obligations; what is submitted is only that the Pseudonymised Data Handler, as defined in section 1, should not be burdened with the obligations of a processor in respect of data that are not personal for it. Moreover, as further illustrated in section 2.5 below, GL § 15 may have the unintended practical consequence of weakening, rather than strengthening, the application and enforcement of the GDPR.

2.3 The rule is incompatible with the text of the GDPR

GL § 15 also appears to be directly incompatible with the provisions of the GDPR that make the application of the Regulation depend on the processing of *personal* data. In particular:

- Article 2(1) GDPR: *"This Regulation applies to the processing of personal data wholly or partly by automated means"*;
- Article 4(2) GDPR: *"'processing' means any operation or set of operations which is performed on personal data or on sets of personal data"*;
- Article 4(8) GDPR: *"'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller"*.

Each of the above provisions presupposes personal data; none of them can apply to an entity for which the data are not personal.

If the GDPR does not apply where the data processed are not personal, GL § 15 turns the transferee of data that are not personal for it into a processor solely because those data are personal for the entity that engaged it. In doing so GL § 15 imposes on that transferee the full set of obligations the GDPR places on processors, although the transferee processes no personal data and is not a processor under the GDPR's own definition in Article 4(8) GDPR: *"'processor' means a natural or legal person, public authority, agency or other body which processes* ***personal data*** *on behalf of the controller"* (the parallel definition in Article 3(12) of Regulation 2018/1725 is identical in substance).

Under the GDPR the processor is burdened with the following obligations:

- to process the data only on documented instructions from the controller, including as regards transfers to third countries (Article 28(3)(a) and Article 29 GDPR), and to inform the controller if an instruction infringes the GDPR (Article 28(3), last subparagraph);
- to ensure that persons authorised to process the data have committed themselves to confidentiality (Article 28(3)(b));
- to take all measures required pursuant to Article 32 GDPR, that is, security measures *"appropriate to the risk"* for the rights and freedoms of natural persons (Article 28(3)(c) and Article 32);
- to engage sub-processors only with the controller's prior authorisation and to flow down the same obligations to them (Article 28(2) and (4));
- to assist the controller in responding to requests from data subjects exercising their rights under Chapter III (Article 28(3)(e));
- to assist the controller in complying with Articles 32 to 36 GDPR, including data protection impact assessments (Article 28(3)(f));
- to delete or return all the personal data at the end of the service (Article 28(3)(g));
- to make available all information necessary to demonstrate compliance and to allow for audits (Article 28(3)(h));
- to maintain a record of all categories of processing activities carried out on behalf of the controller, including the categories of data subjects (Article 30(2));
- to cooperate with the supervisory authority (Article 31);
- to notify the controller without undue delay after becoming aware of a personal data breach (Article 33(2));
- to designate a data protection officer where the conditions of Article 37 are met, and a representative in the Union where Article 27 applies;
- to comply with Chapter V when the data are transferred to a third country (Articles 44 to 49);
- to be liable for damage caused by processing in breach of its obligations (Article 82(2)) and exposed to administrative fines (Article 83(4)(a)).

Several of these obligations can only be performed by an entity that knows whose data it holds: assisting with data subject requests, notifying personal data breaches, recording categories of data subjects, deleting *"personal data"* at the end of the service. An entity for which the data are not personal cannot, by definition, perform them. The qualification as processor, therefore, presupposes personal data and cannot create them. GL § 15 thus produces the paradox of a processor of non-personal data required, under Article 28(3)(c) and Article 32 GDPR, to adopt

security measures *"appropriate to the risk"* to the rights of natural persons, in respect of data that present no identification risk in its hands. The EDPB Guidelines 07/2020 on the concepts of controller and processor, cited in footnote 11 of the Guidelines, likewise presuppose personal data throughout.

2.4 The teleological argument does not support the rule

GL § 15 states that it is justified by a teleological argument, which the Guidelines set out in three points: (1) EU data protection law relies on the concept of processor *"to prevent controllers from avoiding GDPR protections by outsourcing their processing activities to third parties"*; (2) the GDPR *"further reinforces this by placing certain obligations directly on processors"*; and (3) contractual agreements and GDPR obligations *"need to work together to ensure that the processor handles the information in an appropriate manner"*. None of these three points justifies the rule laid down in GL § 15, for the four reasons set out below.

First, the purpose of the processor concept is to ensure that the processing of personal data remains protected when a controller uses others to carry it out. That purpose is fully served under the approach proposed in this feedback, which may be summarised as follows: the controller that pseudonymises the data and holds the key continues to process personal data and remains bound by every GDPR obligation; the Pseudonymised Data Handler, for which the data are not personal because it neither holds nor can obtain the key, is not a processor and is instead bound by the contractual and technical measures the controller imposes on it. Under this approach no safeguard is lost, because every substantive safeguard sits with the controller. The controller is accountable for the Pseudonymised Data Handler's operations because it chose that entity and the measures. What is removed is only a set of obligations imposed on a party that cannot perform them.

Second, the Court in SRB addressed the circumvention risk and chose a different remedy: the data become personal again for any onward transfer to third parties who may reasonably attribute them, and indirectly for the controller (SRB §§ 84-85). The Court in SRB did not say that the Pseudonymised Data Handler becomes a processor. The Guidelines replace the Court's remedy with one the Court did not adopt.

Third, the second and third reasons given in GL § 15 are circular. The GDPR imposes obligations directly on processors because processors process personal data; those obligations cannot be invoked to justify calling an entity a processor when the premise, personal data in its hands, is absent.

Fourth, a teleological reading must follow the Regulation's own logic, which is risk-based (Articles 24, 25, 32 and 35 GDPR; recitals 75-77 GDPR). Recital 28 GDPR

states that *"the application of pseudonymisation to personal data can reduce the risks to the data subjects concerned and help controllers and processors to meet their data-protection obligations"*, and the Court recalls the same idea at SRB § 72. The reasoning is simple. The GDPR calibrates obligations on the risk that a processing operation creates for natural persons. Where the Pseudonymised Data Handler cannot identify anyone, the risk of identification in its hands is *"insignificant"* in the sense of SRB § 82 and AG § 57. A risk-based system therefore attaches no obligations to that entity, not because of a gap in protection, but because there is no risk for the entity's obligations to address. GL § 15 does the opposite: it attaches the full set of processor obligations to an entity whose processing creates no identification risk, and in doing so it deprives robust pseudonymisation of any legal effect for the entity that receives the data.

2.5 The rule makes pseudonymisation pointless

Pseudonymisation is a technique: the Court describes it as *"the establishment of technical and organisational measures to reduce the risk of a data set being correlated with the identity of data subjects"* (SRB § 72). When a controller applies that technique properly and transfers the pseudonymised data to a Pseudonymised Data Handler engaged to process them, the Pseudonymised Data Handler cannot lift the measures unless the controller itself hands it the means to do so. The primary obligation, therefore, lies with the controller: not to disclose the key or the additional information to the Pseudonymised Data Handler. That obligation is written into the very definition of pseudonymisation in Article 4(5) GDPR, which requires that the additional information be *"kept separately"* and be *"subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person"*. The condition set by the Court in SRB § 77, that the Pseudonymised Data Handler is *"not in a position to lift those measures"*, is met precisely when the controller complies with that obligation and does not disclose to the Pseudonymised Data Handler the information that would allow the data subjects to be identified. If, in that situation, the Pseudonymised Data Handler is nevertheless a processor of personal data, pseudonymisation serves no purpose. A controller that must in any event treat the Pseudonymised Data Handler as its processor has no incentive to invest in pseudonymisation before transmitting the data: it can send them in clear text under an Article 28 GDPR contract, saving both the cost of pseudonymisation and the loss of utility it entails. The facts of SRB illustrate the point: why would the SRB have invested in a pseudonymisation architecture, with randomly generated codes and a separate registration database (SRB §§ 22-28), if the transfer to Deloitte had to be treated as a transfer of personal data to a processor regardless of that architecture? Under GL § 15, at least from a purely economic point of view, the SRB would have had no reason to pseudonymise the data at all.

Ultimately, the practical outcome of GL § 15 is the opposite of what its teleological justification is meant to achieve.

Moreover, GL § 15 runs counter to what the EU legislator intended:

- Recital 28 GDPR states that *"the application of pseudonymisation to personal data can reduce the risks to the data subjects concerned and help controllers and processors to meet their data-protection obligations"*;
- recital 29 GDPR states that the Regulation seeks *"to create incentives to apply pseudonymisation when processing personal data"*;
- Articles 25(1) and 32(1)(a) GDPR name pseudonymisation as a measure of data protection by design and of security;
- the Court itself recalls recital 17 of Regulation 2018/1725 to the same effect (SRB § 72).

3. Conclusion

The author is grateful to the EDPB for the opportunity to comment on the Guidelines and for the clarity they bring to the assessment of anonymity. For the reasons set out above, the author respectfully invites the EDPB to reconsider GL § 15 so that an entity which processes pseudonymised data on behalf of a controller, without holding or being able to obtain the information needed to identify the data subjects, is not regarded as a processor of personal data, while the controller remains fully accountable for the outsourced operation.

Paolo Maria Gangi, LL.M.

Paolo Maria Gangi